IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

CYNTHIA WEISENBERGER, individually and on behalf of all others similarly situated, Plaintiff, v. AMERITAS MUTUAL HOLDING COMPANY, Defendant.	)	**Case No. 4:21-cv-3156 (JMG-SMB)** **AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

AMENDED CLASS ACTION COMPLAINT

Plaintiff Cynthia Weisenberger ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Ameritas Mutual Holding Company ("Ameritas" or "Defendant"). Based upon personal knowledge as well as information and belief, Plaintiff specifically alleges as follows:

NATURE OF THE ACTION

1. This is a class action for damages with respect to Ameritas Mutual Holding Company, for its failure to exercise reasonable care in securing and safeguarding their customers' sensitive personal data— including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, and policy numbers, collectively known as personally identifiable information ("PII" or "Private Information").

2. This class action is brought on behalf of customers whose sensitive PII was stolen by cybercriminals in a cyber-attack that accessed customer date through Ameritas's services on or around May 1–June 4, 2019 (the "Data Breach").

3. The Data Breach affected at least 39,675 individuals from Ameritas services.

4. Ameritas reported to Plaintiff information compromised in the Data Breach included her PII.

5. Plaintiff was not notified until August 13, 2019, three months after her information was first accessed.

6. As a result of the Data Breach, Plaintiff has experienced various types of misuse regarding her PII over a two-year period, including unauthorized credit card charges, unauthorized access to her email accounts, fraudulent four credit cards closed over a period of two years, and consistent spam emails.

7. Plaintiff has mitigated harm by reporting the theft to the police and filing an FTC fraud report that reported her identity theft to the FTC.

8. There has been no assurance offered from Ameritas that all personal data or copies of data have been recovered or destroyed. Ameritas offered Kroll credit monitoring, which does not guarantee security of Plaintiff's information. In order to mitigate further harm, Plaintiff chose not to disclose any more information to receive services connected with Ameritas.

9. Accordingly, Plaintiff asserts claims for violations of negligence, an intrusion upon seclusion, breach of implied contract, breach of fiduciary duty, breach of Nebraska Consumer Protection Act ("CPA"), Nebraska Revised Statutes § 59-1601, *et seq*., and a violation of the Nebraska Uniform Deceptive Trade Practices Act ("UDTPA"), Nebraska Revised Statutes §§ 87-301, *et. seq*.

PARTIES

Plaintiff Cynthia Weisenberger

10. Plaintiff Cynthia Weisenberger is a resident of North Carolina and brings this action in her individual capacity and on behalf of all others similarly situated. Weisenberger paid

Defendant over $40 a month over a period of at least three years to receive a dental insurance policy from Defendant. To receive the dental insurance policy, Defendant required her to disclose her PII, which it expressly and impliedly promised to safeguard. Defendant, however, did not take proper care of Weisenberger's PII, leading to its exposure as a result of Defendant's inadequate data security. In April 2019, Weisenberger received a notification letter from Defendant stating that her PII was taken, which included, "names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, and policy numbers." The letter also advised Weisenberger to contact the Federal Trade Commission. In response to the recommendation, Weisenberger put a fraud alert on her information through the FTC. Additionally, Weisenberger reported the leak to her local police department. The police could not help her due to the high volume of data breach reports they consistently receive.

11. The letter also offered one year of credit monitoring through Kroll, which was ineffective for Weisenberger and class members. The Kroll credit monitoring would have shared her information with third parties and could not guarantee complete privacy of her sensitive PII.

12. In the two years following the breach, Weisenberger has experienced a slew of harms as a result of the Data Breach. She lost $280 due to fraudulent activity on her Amazon account that was not refunded, her bank had to replace her credit cards five times (including most recently in July) due to fraudulent charges, and two of her email accounts were compromised. She has also received targeted advertising for credit monitoring. To mitigate further harm, she has followed the Federal Trade Commission's advice and put a fraud alert on her credit report.

Defendant

13. Defendant Ameritas Mutual Holding Company is a Nebraska insurance company., which operates nationally, including in North Carolina. Ameritas offers multiple products, including dental insurance. Ameritas is the marketing name for subsidiaries of Ameritas Mutual Holding Company, including but not limited to, Ameritas Life Insurance Corp. Ameritas registered its headquarters at 5900 O Street, Lincoln, NE 68510. Ameritas' corporate policies and practices, including those for data privacy and those that led to the Data Breach, were established in, and emanated from, Nebraska.

14. Ameritas closed its 2019 revenue with $2.5 billion in total revenue, a 5% increase from their previous year.[1]

JURISDICTION AND VENUE

15. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

14. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

15. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

[1] Ameritas, *2019 Annual* Report 2 (2020), https://www.ameritas.com/OCM/GetPDF?pdfname=511305.

FACTS

16. Defendant provides insurance to tens of thousands of customers in North Carolina and about five million customers across the country. As part of its business, Defendant stores a vast amount of its customers' Private Information. In doing so, Defendant was entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable laws.

17. In May of 2019, Defendant first learned of unauthorized entry into its network, which contained customers' Private Information including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, and policy numbers.

18. Upon learning of the Data Breach in May 2019, Defendant investigated. As a result of the Data Breach, Defendant initially estimated that the Private Information of 39,675 customers were potentially compromised stemming from services previously received.

19. In May 2019 Defendant announced that it first learned of suspicious activity that allowed one or more cybercriminals to access their systems through a phishing attack. The 2019 Notice disclosed that a phishing campaign enabled a threat actor to access Ameritas systems.

20. Defendant admitted that "several associates" at different points in time between May and June 2019 gave hackers their email credentials, compromising a large number of email inboxes.

21. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected customers, which resulted in Plaintiff and class members suffering harm they otherwise could have avoided had a timely disclosure been made.

22. Ameritas's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its employees' e-mail accounts, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach was a system-wide breach, whether servers storing information were accessed, and how many patients were affected by the Data Breach. Even worse, Ameritas offered only a single year of identity monitoring to Plaintiff and class members, which required the disclosure of additional PII that Ameritas had just demonstrated it could not be trusted with.

23. Plaintiff and class members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff's and class members' unencrypted, unredacted information, including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, policyholder names, employer names, policy numbers name, and more.

24. The Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

25. Defendant disregarded the rights of Plaintiff and class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and class members was compromised through unauthorized access by an unknown third party. Plaintiff and class members have a continuing interest in ensuring that their information is and remains safe.

Defendant's Privacy Promises

26. Ameritas made, and continues to make, various promises to its customers, including Plaintiff, that it will maintain the security and privacy of their Private Information.

27. In a packet of materials explaining dental benefits from 2018, Ameritas encouraged customers, including Plaintiff, to register for an online member account. In doing so, Ameritas said: "Using online services helps to minimize your risk of identity theft, protect your privacy and get your benefit information faster than through the mail."

28. In its HIPAA Notice of Privacy Practices for Ameritas Group Dental, Vision and Hearing Care members, which has not been revised since August 31, 2017,[2] and was therefore applicable to Plaintiff, Defendant stated under a section bolded and titled "our responsibilities," the following:

- "We are required by law to maintain the privacy and security of your protected health information."
- "We will let you know promptly if a breach occurs that may have compromised the privacy or security of your information."
- "We must follow the duties and privacy practices described in this Notice, and give you a copy of it."

[2] Ameritas, *Your Information. Your Rights. Our Responsibilities.* (2017), https://www.ameritas.com/OCM/GetFile?doc=381698.

- "We will not use or share your information other than as described in this Notice, unless you tell us we can in writing."

29. Ameritas describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

30. By failing to protect Plaintiffs' and class members' Private Information, and by allowing the Data Breach to occur, Ameritas broke these promises to Plaintiffs and class members.

Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Customers' Private Information

31. Ameritas acquires, collects, and stores a massive amount of its customers' protected PII, including health information and other personally identifiable data.

32. As a condition of engaging in health-related services, Ameritas requires that these customers entrust them with highly confidential Private Information.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class members' Private Information, Ameritas assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and class members' Private Information from disclosure.

34. Defendant had obligations created by the Health Insurance Portability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), industry standards, common law, and representations made to class members, to keep class members' Private Information confidential and to protect it from unauthorized access and disclosure.

35. Defendant failed to properly safeguard Plaintiff and class members' Private Information, allowing hackers to access their Private Information.

36. Plaintiff and class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligations to keep such information confidential and secure from unauthorized access.

37. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

38. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

39. In fact, Defendant has been on notice for years that the healthcare industry and health insurance companies are a prime target for scammers because of the amount of confidential customer information maintained.

40. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[3]

[3] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

41. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[4]

42. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[5] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[6] That trend continues.

43. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[7] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[8] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty

[4] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[5] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[6] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[7] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.

[8] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[9]

44. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

45. Healthcare related data breaches continued to rapidly increase into 2019 when Ameritas was breached.[10]

46. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[11]

47. The report from Proofpoint was published March 27, 2019, and summarized findings of recent healthcare industry cyber threat surveys and recounted good, common sense steps that the targeted healthcare companies should follow to prevent email-related cyberattacks.

48. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's on-going training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done

[9] *Id.*

[10] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

[11] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishingstatistics-2019-himss-survey-results.

through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[12]

49. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies without the heightened standard of care applicable in the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of its Book guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[13]

50. The guidance that ProtonMail provides non-healthcare industry small businesses is likely still not adequate for an insurance company like Ameritas, with the heightened healthcare standard of care based on HIPAA, and the increased danger from the sensitivity and wealth of Private Information it retains, but ProtonMail's guidance is informative for showing how inadequately Ameritas protected the Private Information of the Plaintiffs and class members. ProofPoint lists numerous tools under the heading, "How to Prevent Phishing":

> a. **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. This training should be continuous as well. . . ."

[12] *Id.*

[13] *The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019), https://protonmail.com/it-security-complete-guide-for-businesses.

b. **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . .

c. **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

d. **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment. . . ."

e. **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f. **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL." [Proofpoint notes that there are tools online available for retrieving original URLs from shortened ones.].

g. **If in doubt, investigate:** "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

h. **Take preventative measures:** "Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."

51. These are basic, common-sense email security measures that every business, not only insurance or other healthcare businesses, should be doing. Ameritas, with its heightened

standard of care should be doing even more. But by adequately taking these common-sense solutions, Ameritas could have prevented this Data Breach from occurring.

52. Charged with handling sensitive PII including healthcare information, Ameritas knew, or should have known, the importance of safeguarding its customers Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Ameritas's patients as a result of a breach. Ameritas failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

53. Indeed, that several of Ameritas' employees, at different points in time, gave away their email credentials demonstrates Ameritas' inadequate employee training to prevent phishing attacks.

54. With respect to training, Ameritas specifically failed to:

a. Implement a variety of anti-phishing training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;

b. Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and

c. Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

55. The PII was also maintained on Ameritas' computer system in a condition vulnerable to cyberattacks such as through the infiltration of Ameritas' employee email accounts. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiff's and class

members' PII was a known risk to Ameritas, and thus Ameritas was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

The Monetary Value of Privacy Protections and Private Information

56. The fact that Plaintiff's and class members' Private Information was stolen—and is likely presently offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

57. At all relevant times, Defendant was well aware that the Private Information it collects from Plaintiff and class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

58. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[14] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive health information on multiple underground Internet websites, commonly referred to as the dark web.

59. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[15]

[14] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[15] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

60. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[16]

61. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[17]

62. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[18] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

63. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their

[16] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, THE WALL STREET JOURNAL (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274 [hereinafter *Web's New Hot Commodity*].

[17] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[18] *Web's Hot New Commodity*, *supra* note 16.

data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[19]

64. The value of Plaintiff and class members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[20] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

65. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[21]

66. The ramifications of Ameritas's failure to keep its patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

[19] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[20] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

[21] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.

67. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[22] This gives thieves ample time to seek multiple treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[23]

68. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[24] Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[25] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[26]

[22] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[23] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[24] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, (2019) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[25] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.

[26] *Id.*

69. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the medical industry and related industries.

70. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the phishing attack into their systems and, ultimately, the theft of their customers' Private Information.

71. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[27] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[28] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and class members that was misused.

[27] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[28] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

72. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

73. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

74. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

75. Acknowledging the damage to Plaintiff and class members, Defendant instructed customers like Plaintiff to "regularly review the statements that you receive from your healthcare insurers and providers. If you identify services that you did not receive, please contact the insurer or provider immediately." Plaintiff and the other class members now face a greater risk of identity theft.

76. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

Ameritas's Conduct Violated HIPAA

77. HIPAA requires covered entities like Ameritas protect against reasonably anticipated

threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[29]

78. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

79. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[30]

80. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. Ameritas's security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only

[29] *What is Considered Protected Health Information Under HIPAA?*, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

[30] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by their workforce in violation of 45 C.F.R. §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

i. Failing to effectively train all members of their workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to

carry out their functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

Ameritas Failed to Comply with FTC Guidelines

81. Ameritas was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

82. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[32] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

[31] *Start With Security: A Guide for Business*, FED. TRADE. COMM'M (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[32] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

84. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[33]

85. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

86. Ameritas failed to properly implement basic data security practices. Ameritas's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

87. Ameritas was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. Ameritas was also aware of the significant repercussions that would result from its failure to do so.

[33] *Start with Security*, *supra* note 31.

Ameritas Failed to Comply with Healthcare Industry Standards

88. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[34]

89. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

90. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of value of the Private Information which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[35] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

91. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Ameritas chose to ignore them. These best practices were known, or should have been known by Ameritas, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

[34] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

[35] *See, e.g., 10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.

Damages to Plaintiff and the Class

92. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

93. The ramifications of Ameritas's failure to keep patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[36]

94. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

95. Defendant further owed and breached its duty to Plaintiffs and class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

96. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff's and class members' Private Information as detailed above, and Plaintiffs are now at a heightened and increased risk of identity theft and fraud.

97. The risks associated with identity theft are serious. While some identity theft victims can

[36] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

98. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, medical services billed in their name, and similar identity theft.

99. Plaintiff and class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

100. Plaintiff and class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with Ameritas. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

101. Plaintiff and class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

102. Plaintiff and members of the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

103. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration

("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[37] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[38] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[39]

104. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[40]

105. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the insurance context, Private Information can be used to submit false insurance claims. As a result, Plaintiff and class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiff and class members, this risk creates unending feelings of fear and annoyance.

[37] *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

[38] *Id.*

[39] *Id.*

[40] *Id.*

Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

106. As a result of the Data Breach, Plaintiff and class members' Private Information has diminished in value.

107. The Private Information belonging to Plaintiff and class members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff or class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

108. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff's and class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

109. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

110. Defendant did not properly train their employees to identify and avoid phishing attempts.

111. Had Defendant remedied the deficiencies in their data security systems and

adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff and class members' Private Information.

112. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

113. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[41]

114. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiff and class members other than telling them to simply do the following:

- "remain vigilant for incidents of fraud and identity theft";
- "review[] account statements and monitor[] your credit report for unauthorized activity";
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

[41] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff and class members' Private Information.

115. Defendant's failure to adequately protect Plaintiff and class members' Private Information has resulted in Plaintiff and class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Ameritas's Data Breach Notice indicates, it is putting the burden on Plaintiff and class members to discover possible fraudulent activity and identity theft.

116. While Defendant offered one year of credit monitoring, Plaintiff could not trust a company that had already breached her data. The credit monitoring offered from Kroll does not guarantee privacy or data security for Plaintiff who would have to expose her information once more to get monitoring services. Thus, to mitigate harm, Plaintiff and class members are now burdened with indefinite monitoring and vigilance of their accounts. For example, Plaintiff caught $280 of fraud charged to her Amazon account because she was vigilant, but despite her vigilance, she was not reimbursed for her loss from the fraud.

117. Moreover, the offer of 12 months of identity monitoring to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent

identity theft.[42] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.[43]

118. Plaintiff and class members have been damaged in several other ways as well. Plaintiff and class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiff and class members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and class members also suffered a loss of the inherent value of their Private Information.

119. The Private Information stolen in the Data Breach can be misused on its own, or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

120. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and class members have suffered, will suffer, and are at increased risk of suffering:

[42] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and class members; and

f. Anxiety and distress resulting fear of misuse of their Private Information.

121. In addition to a remedy for the economic harm, Plaintiff and class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

122. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

123. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class") pursuant to Federal Rule of Civil Procedure 23.

124. Plaintiff proposes the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Class:

> All persons whose Private Information was compromised as a result of the Data Breach discovered on or about May 2019 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

125. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

126. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all class members would be impracticable. On information and belief, the Nationwide Class number in the thousands.

127. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

b. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

e. Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

g. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

h. Whether Defendant was unjustly enriched by its actions; and

i. Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

128. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

129. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

130. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because their interests do not conflict with the interests of the Classes they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

131. **Injunctive Relief-Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

132. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All class members)

133. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

134. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

135. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

136. Defendant owed numerous duties to Plaintiff and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

137. Defendant also breached their duty to Plaintiff and class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to

unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

138. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

139. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and class members' Private Information.

140. Defendant breached their duties to Plaintiff and class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and class members' Private Information.

141. Because Defendant knew that a breach of their systems would damage thousands of their customers, including Plaintiff and class members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

142. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach.

143. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

144. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

145. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

146. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

147. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to class members' Private Information;

d. Failing to detect in a timely manner that class members' Private Information had been compromised; and

e. Failing to timely notify class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

148. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff's and class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and class members' Private Information during the time it was within Defendant's possession or control.

149. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and class members with timely notice that their sensitive Private Information had been compromised.

150. Neither Plaintiff nor the other class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

151. As a direct and proximate cause of Defendant's conduct, Plaintiff and class members suffered damages as alleged above.

152. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all class members.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and All class members)

153. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

154. Plaintiff and other class members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide insurance and, impliedly, if not explicitly, agreed to protect Plaintiff and class members' Private Information.

155. These contracts include HIPAA privacy notices and explanation of benefits documents.

156. To the extent Defendant's obligation to protect Plaintiffs' and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other class members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. No Plaintiff would have entered into these contracts with Defendant without understanding that Plaintiffs' and other class members' Private Information would be

safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

157. A meeting of the minds occurred, as Plaintiff and other class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

158. The protection of Plaintiff and class members' Private Information were material aspects of Plaintiff's and class members' contracts with Defendant.

159. Defendant's promises and representations described above relating to HIPAA and industry practices, and about Defendant' purported concern about their clients' privacy rights became terms of the contracts between Defendant and their clients, including Plaintiff and other class members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

160. Plaintiff and class members read, reviewed, and/or relied on statements made by or provided by Ameritas and/or otherwise understood that Ameritas would protect its patients' Private Information if that information were provided to Ameritas.

161. Plaintiff and class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

162. As a result of Defendant's breach of these terms, Plaintiffs and other class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with

credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

163. Plaintiff and class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and All class members, in the Alternative to Count II)

164. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

165. Through their course of conduct, Defendant, Plaintiff, and class members entered into implied contracts for the provision of insurance, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and class members' Private Information.

166. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into insurance agreement with Defendant.

167. The valid and enforceable implied contracts to provide insurance services that Plaintiff and class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

168. When Plaintiff and class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

169. Defendant solicited and invited class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and class members accepted Defendant's offers and provided their Private Information to Defendant.

170. In entering into such implied contracts, Plaintiff and class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

171. class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

172. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide insurance to Plaintiff and class members; and (b) protect Plaintiff's and the class members' Private Information provided to obtain such benefits of insurance policy. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

173. Both the provision of insurance and the protection of Plaintiff's and class members' Private Information were material aspects of these implied contracts.

174. The implied contracts for the provision of insurance services – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and class members' Private Information- are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

175. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and protect the privacy of Plaintiff's and class members Private Information.

176. Consumers of insurance value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining insurance private. To customers such as Plaintiff and class members, insurance that does not adhere to industry standard data security. Plaintiff and class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected, or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

177. A meeting of the minds occurred, as Plaintiff and class members agreed and provided their Private Information to Defendant and/or its affiliated healthcare providers, and paid for the provided insurance in exchange for, amongst other things, both the provision of healthcare and insurance services and the protection of their Private Information.

178. Plaintiff and class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

179. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

180. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and class members Private Information as evidenced by its notifications of the Data Breach to Plaintiff and class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and class members private information as set forth above.

181. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

182. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiff and class members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

183. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, class members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated providers.

184. As a direct and proximate result of the Data Breach, Plaintiff and class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future,

disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

185. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

186. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all class members.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All class members)

187. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

188. In light of their special relationship, Defendant have become the guardian of Plaintiff's and Class Members' Private Information. Defendants have become a fiduciary, created by its undertaking and guardianship of patients' Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' Private Information and to timely notify them in the event of a data breach.

189. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship. Defendant breached its fiduciary duties owed to Plaintiff and class members by failing to do the following:

a. Properly encrypt and otherwise protect the integrity of the system containing Plaintiff's and class members' Private Information;

b. Timely notify and/or warn Plaintiff and class members of the Data Breach;

c. ensure the confidentiality and integrity of electronic protected health information Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R 164.306(a)(1);

d. implement technical policies and procedures to limit access to only those persons or software programs that have been granted access rights in violation of 45 C.F.R 164.312(a)(1);

e. implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R 164.308(a)(1);

f. identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R 164.308(a)(6)(ii);

g. protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R 164.306(a)(2);

h. protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R 164.306(a)(3);

i. ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R 164.306(a)(94);

j. prevent the improper use and disclosure of protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R 164.502, *et seq*.;

k. effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforce to carry out their functions and to maintain security of protected health information in violation of 45 C.F.R 164.530(b) and 45 C.F.R 164.308(a)(5);

l. design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R 164.530(c); and otherwise failing to safeguard Plaintiff's and class members' Private Information.

190. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its

continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

191. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Breach of Nebraska Consumer Protection Act ("CPA"), Nebraska Revised Statutes § 59-1601, *et seq*.,
(On Behalf of Plaintiff and All class members)

192. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

193. Plaintiff, class members, and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Consumer Protection Act ("CPA"), Neb. Rev. Stat. § 59-1601, et seq.

194. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violation of the CPA, including but not limited to:

1. representing that its services were of a particular standard or quality that it knew or should have known were of another;

2. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and class members' Private Information, which was a direct and proximate cause of the Data Breach;

3. Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

4. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

5. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and class members' Private Information, including by implementing and maintaining reasonable security measures;

6. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information; and

7. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and class members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Security breach.

195. Defendant's representations and omissions were material because it was likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

196. In addition, Defendant's failure to secure consumers' Personal Information violated the FTCA and HIPAA and therefore violates the CPA.

197. Also, Defendant's failure to give timely notice of this Data Breach in violation of Nebraska's notification of security breach statute, Neb. Rev. Stat. § 87-801 et seq is an unfair or deceptive act pursuant to Neb. Rev. Stat. § 87-808, and therefore violates the Consumer Protection Act.

198. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

199. The aforesaid conduct constitutes a violation of the CPA, Neb. Rev. Stat. § 59-1603, in that it is a restraint on trade or commerce.

200. These violations have caused financial injury to the Plaintiff and the other class members.

201. The Defendant's violations of the CPA have an impact of great and general importance on the public, including Nebraskans. Tens of thousands of Nebraskans have been insured by Ameritas, an appreciable number of whom have been impacted by the Data Breach. In addition, Nebraska residents have a strong interest in regulating the conduct of its corporate citizens such as Ameritas, whose policies and practices described herein affected tens of thousands across the country.

202. As a direct and proximate result of Defendant's violation of the CPA, Plaintiff and class members are entitled to a judgment under Neb. Rev. Stat. § 59-1609 to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

COUNT VI
VIOLATION OF NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Nebraska Revised Statutes § 87-301, et seq.
(On Behalf of Plaintiff and class members)

203. Plaintiff, all class members and Defendant each qualify as a person engaged in trade or commerce as contemplated by the Nebraska Uniform Deceptive Trade Practices Act ("UDTPA"), Neb. Rev. Stat. § 87-301, et seq.

204. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and class members' Private Information constitute representations as to characteristics, uses, or benefits of services that such services did not actually have, in violation of Neb. Rev. Stat. § 87-302(a)(5).

205. On information and belief, Ameritas formulated and conceived of the systems it used to compile and maintain patient information largely within the state of Nebraska, oversaw its data privacy program complained of herein from Nebraska, and its communications and other efforts related to the Data Breach largely emanated from Nebraska.

206. Most, if not all, of the alleged misrepresentations and omissions by Ameritas complained of herein that led to inadequate safety measures to protect patient information occurred within, or were approved within, Nebraska.

207. Defendant's implied and express representations that it would adequately safeguard Plaintiff's and class members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Neb. Rev. Stat. § 87-302(a)(8).

208. Defendant knowingly made false or misleading statements regarding the use of personal information submitted by members of the public in that Defendant advertised it is committed to

protecting privacy and securely maintaining personal information. Defendant did not securely maintain personal information as represented, in violation of Neb. Rev. Stat. § 87-302(a)(15).

209. These violations have caused financial injury to Plaintiff and class members and have created an unreasonable, imminent risk of future injury.

210. Accordingly, Plaintiff, on behalf of herself and class members, bring this action under the Uniform Deceptive Trade Practices Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety; to disclose with specificity the type of PII compromised during the Data Breach; and to routinely and continually conduct training to inform internal security personnel how to prevent, identify, and contain a breach, and how to appropriately respond;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiff and the Classes;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

Date: November 3, 2021

Respectfully submitted,

/s/ Jason S. Rathod
Jason S. Rathod*
jrathod@classlawdc.com
Nicholas A. Migliaccio*
nmigliaccio@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

Vincent M. Powers Bar No. 15866
POWERS LAW
411 South 13th Street, Suite 300
Lincoln, NE 68508
Tel: (402) 474-8000
powerslaw@me.com

*Permanently Admitted to Practice in D. Neb.

CERTIFICATE OF SERVICE

I, Jason Rathod, hereby certify that on November 3, 2021, a true and correct copy of the foregoing Amended Class Action Complaint was electronically filed with the Clerk of the Court by using the CM/ECF system, which sends notice to all counsel of record.

/s/ Jason S. Rathod
Jason S. Rathod